CLAIMS

What is claimed is:

1. A method comprising:

associating a security association with a traffic stream;

associating a metric value with the security association;

modifying the metric value based on network traffic; and

dynamically mapping the traffic stream to one of multiple components that perform cryptography operations based on the metric value.

2. The method of claim 1 wherein the dynamic mapping is performed using a time-based analysis.

3. The method of claim 1 wherein the multiple components comprise a driver agent and a network interface.

4. The method of claim 1 wherein dynamically mapping traffic streams to one of multiple components comprises selecting between performing cryptography operations with a driver agent and performing cryptography operations with a network interface using cached cryptography information.

5. The method of claim 1 wherein the dynamic mapping further comprises replacing a cached security association with a non-cached security association when the metric value of the

non-cached security association differs from the metric value of the cached security association by at least a predetermined amount.

6. The method of claim 5 wherein the predetermined amount is selected based on a cost-based analysis.

7. The method of claim 1 wherein modifying the metric value further comprises initializing the metric to a predetermined value when the security association is received by a driver agent.

8. The method of claim 1 wherein modifying the metric value further comprises changing the associated metric value by a predetermined amount when the security association is added to a cache.

9. The method of claim 1 wherein modifying the metric value further comprises changing the associated metric value when a packet is received.

10. The method of claim 1 wherein modifying the metric value further comprises periodically changing the metric value independent of network traffic.

11. An apparatus comprising:

a network interface coupled to receive network traffic streams; and

a driver agent coupled to communicate with the network interface, the driver agent to associate a security association with a traffic stream, associate a metric value with the security association, modify the metric value based on network traffic, and dynamically map the traffic stream to one of multiple components that perform cryptography operations based on the metric value.

12. The apparatus of claim 11 wherein the dynamic mapping is performed using a time-based analysis.

13. The apparatus of claim 11 wherein the multiple components comprise a driver agent and a network interface.

14. The apparatus of claim 11 wherein dynamically mapping traffic streams to one of multiple components comprises selecting between performing cryptography operations with a driver agent and performing cryptography operations with a network interface using cached cryptography information.

15. The apparatus of claim 11 wherein the dynamic mapping further comprises replacing a cached security association with a non-cached security association when the metric value of the non-cached security association is greater than the metric value of the cached security association by at least a predetermined amount.

16. The apparatus of claim 15 wherein the predetermined amount is selected based on a cost-based analysis.

17. The apparatus of claim 11 wherein modifying the metric value further comprises initializing the metric to a predetermined value when the security association is received by a driver agent.

18. The apparatus of claim 11 wherein modifying the metric value further comprises changing the associated metric value by a predetermined amount when the security association is added to a cache.

19. The apparatus of claim 11 wherein modifying the metric value further comprises changing the associated metric value when a packet is received.

20. The apparatus of claim 11 wherein modifying the metric value further comprises periodically changing the metric value independent of network traffic.

21. An article comprising a machine-accessible medium to provide machine-readable instructions that, when executed, cause one or more electronic systems to:

associate a security association with a traffic stream;

associate a metric value with the security association;

modify the metric value based on network traffic; and

dynamically map the traffic stream to one of multiple components that perform cryptography operations based on the metric value.

22. The article of claim 21 wherein the dynamic mapping is performed using a time-based analysis.

23. The article of claim 21 wherein the multiple components comprise a driver agent and a network interface.

24. The article of claim 21 wherein dynamically mapping traffic streams to one of multiple components comprises selecting between performing cryptography operations with a driver agent and performing cryptography operations with a network interface using cached cryptography information.

25. The article of claim 21 wherein the dynamic mapping further comprises replacing a cached security association with a non-cached security association when the metric value of the non-cached security association is greater than the metric value of the cached security association by at least a predetermined amount.

26. The article of claim 25 wherein the predetermined amount is selected based on a cost-based analysis.

27. The article of claim 21 wherein modifying the metric value further comprises initializing the metric to a predetermined value when the security association is received by a driver agent.

28. The article of claim 21 wherein modifying the metric value further comprises changing the associated metric value by a predetermined amount when the security association is added to a cache.

29. The article of claim 21 wherein modifying the metric value further comprises changing the associated metric value when a packet is received.

30. The article of claim 21 wherein modifying the metric value further comprises periodically changing the metric value independent of network traffic.

31. A electronic data signal embodied in a data communications medium shared among a plurality of network devices comprising sequences of instructions that, when executed, cause one or more electronic systems to:

associate a security association with a traffic stream;

associate a metric value with the security association;

modify the metric value based on network traffic; and

dynamically map the traffic stream to one of multiple components that perform cryptography operations based on the metric value.

32. The electronic data signal of claim 31 wherein the dynamic mapping is performed using a time-based analysis.

33. The electronic data signal of claim 31 wherein the multiple components comprise a driver agent and a network interface.

34. The electronic data signal of claim 31 wherein dynamically mapping traffic streams to one of multiple components comprises selecting between performing cryptography operations with a driver agent and performing cryptography operations with a network interface using cached cryptography information.

35. The electronic data signal of claim 31 wherein the dynamic mapping further comprises replacing a cached security association with a non-cached security association when the metric value of the non-cached security association is greater than the metric value of the cached security association by at least a predetermined amount.

36. The electronic data signal of claim 35 wherein the predetermined amount is selected based on a cost-based analysis.

37. The electronic data signal of claim 31 wherein modifying the metric value further comprises initializing the metric to a predetermined value when the security association is received by a driver agent.

38. The electronic data signal of claim 31 wherein modifying the metric value further comprises changing the associated metric value by a predetermined amount when the security association is added to a cache.

39. The electronic data signal of claim 31 wherein modifying the metric value further comprises changing the associated metric value when a packet is received.

40. The electronic data signal of claim 31 wherein modifying the metric value further comprises periodically changing the metric value independent of network traffic.

41. A method comprising:

associating a security association with a traffic stream;

determining whether the security association necessary for performing cryptography operations on the packet is cached;

determining whether the security association should be cached based on a predetermined policy; and

caching the security association if it is determined from the predetermined policy that the security association should be cached.

42. The method of claim 41 wherein the predetermined policy is performed on a periodic basis.

43. The method of claim 41 wherein the predetermined policy comprises:

associating a metric value with a security association;

initializing the metric value to a predetermined value when the security association is received by a driver agent;

increasing the value of the security association metric by a predetermined value when the associated security association is added to a cache;

incrementing the value of the associated security association metric when a packet is received; and

determining whether the metric value is greater than the lowest metric value of cached security associations by at least a predetermined amount.

44. The method of claim 43 further comprising periodically decreasing the metric value.